



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/707,408	12/11/2003	David L. Kaminsky	014682.000002	1407
44870 7590 01/23/2008 MOORE & VAN ALLEN, PLLC For IBM P.O. Box 13706 Research Triangle Park, NC 27709			EXAMINER MADAMBA, GLENFORD J	
			ART UNIT 2151	PAPER NUMBER
			MAIL DATE 01/23/2008	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.		Applicant(s)	
	10/707,408		KAMINSKY ET AL.	
	Examiner		Art Unit	
	Glenford Madamba		2151	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 01 November 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3,6-15,18-29,31-38 and 40-44 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-3,6-15, 18-29, 31-38, and 40-44 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Remarks and Amendments

1. This action is in response to remarks and claim amendments filed by Applicant's representative on November 1, 2007.
2. Applicant's remarks and claim amendments filed on November 1, 2007 have been considered but are now moot in light of the new grounds of rejection provided with this action.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1- 5, 10-17, 23-31, and 35-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shanumgam et al (hereinafter Shanumgam), U.S. Patent US 7,032,022 B1 in view of Menditto et al (hereinafter Menditto), U.S. Patent 6,981,029.

As per Claims 1, 11, 12, 23, 24 and 36, Shanumgam in view of Menditto discloses a method to distribute policies, comprising [Abstract]:

determining if a policy template is present at an enforcement point (Policy Enforcers 142 / 126) [Fig. 1] [col 1, L65 – col 2, L26] in response to receiving an identification (ID) (i.e., Policy Identifier {ID}) [col 10, L53] assigned to the policy template at the enforcement point; (Menditto)

transmitting a query from the enforcement point to a repository, where policy templates are stored, in response to the policy template not being present at the enforcement point, wherein the query includes the ID assigned to the policy template; (Menditto)

receiving the policy template at the enforcement point, wherein the policy template is transmitted by the repository in response to the query; (Menditto) and

receiving a set of parameters (i.e., attributes) [col 19, L49-65] to be used in the policy template (e.g., selected policy enforcer 'settings') [Abstract] [Fig. 5] [col 8, L20-54] at the enforcement point (i.e., 411) [Fig. 5] [Figs. 1-4, 13-14 & 17] [col 1, L65 – col 2, L26].

While Shanumgam discloses substantial features of the invention, such as Policy Server Database 130, Policy Enforcement Points 124 / 126, Policy Settings for the Policy Enforcers, and Policy Identifier (ID) Attribute 724 for identifying a particular policy rule in the list of policies, and a method of distributing / replicating the 'policies' (including their Policy ID) from Policy Server to Policy Enforcers 124 / 126, the additionally recited features of the method comprising the steps of determining if a policy template is present at an enforcement point in response to receiving an identification (ID) assigned to the policy template at the enforcement point; transmitting a query from the enforcement point to a repository, where policy templates are stored, in response to the policy template not being present at the enforcement point, wherein the query includes the ID assigned to the policy template; and receiving the policy template at the enforcement point, wherein the policy template is transmitted by the repository in response to the query are disclosed by Menditto in a related endeavor.

Menditto discloses as his invention an information service provider network that includes a content gateway to process requests for information from a client terminal. The content gateway includes a router for receiving a request for information from the client terminal. The router forwards the request according to the domain name to a selected one of a plurality of processors to further process the request. The selected one of the plurality of processors identifies an information source to satisfy the request in response to the additional content of the request [Abstract] [col 1, L45-53] [Figs. 1 & 3]. As part of his invention, Menditto discloses that "Content Gateways 18 distribute information from content providers 14 either directly or through content delivery nodes

22 to client terminals 16 according to Content Gateway Policy Manager 26 (CGPM).

CGPM 26 is a management node in information service provider 12 that serves as a repository for content policies and communicates with content gateways 18 to distribute content policies within information service provider 12 and exchange policies with other CGPMs in other information service providers" [col 2, L43-53].

In particular, Menditto discloses the additionally recited features of the method comprising the steps of determining if a policy template is present at an enforcement point in response to receiving an identification (ID) assigned to the policy template at the enforcement point; transmitting a query from the enforcement point to a repository, where policy templates are stored, in response to the policy template not being present at the enforcement point, wherein the query includes the ID assigned to the policy template; and receiving the policy template at the enforcement point, wherein the policy template is transmitted by the repository in response to the query [col 3, L1-29][col 6, L16-53] (e.g., "...content policy may be *downloaded* to content gateway 18 *on-demand*....") [col 7, L1-53] [col 8, L27-30] (e.g., "...content policy associated with a query...receiving policy updates from CGPM 26 and processing subsequent requests according to the newly installed policy.) [col 9, L37-62] [col 12, L20 –col 13, L6].

It would thus be obvious to one of ordinary skill in the art at the time of the invention to combine and/or modify Shanumgam's invention with the above said additionally recited features, as disclosed by Menditto for the motivation of providing systems and method for processing a request for information in a network that has considerable advantages over conventional routing techniques (e.g. determining a

source of information based on the additional content of a request apart from the domain name associated therewith) [col 1, L54 – col 2, L2].

Claims 11, 12, 23, 24 and 36 recite the same limitations as claim 1, are distinguished only by statutory category, and thus rejected on the same basis.

As per Claims 2, 13, 29 and 37, Shanumgam discloses the method of claim 1, binding the parameters to the policy template [Abstract] [Figs. 5 & 17] [col 20, L22-47].

As per Claims 3, 14 and 38, Shanumgam discloses the method of claim 2, further comprising implementing the policy associated with the policy template [Figs. 1-5, 15 & 17] [col 1, L65 – col 2, L26].

As per Claim 15, Shanumgam discloses the method of claim 11, further comprising storing each one of the at least one set of parameters by name and type [col 13, L24-30].

As per Claims 31 and 40, Shanumgam discloses the method of claim 1, further comprising transmitting any policy templates to the enforcement point or any of the selected enforcement points in response to a query from the enforcement point or any of the selected enforcement points including any IDs assigned to the policy templates.

As per Claims 10, 28 and 35, Shanumgam in view of Menditto discloses a method to distribute policies, comprising:

defining a policy template associated with each policy; assigning a unique identification (ID) to each policy template [Abstract];

storing each policy template and assigned ID (130) [Fig. 1]; and

transmitting only the assigned ID to an enforcement point for each policy to be enforced by the enforcement point, wherein only the ID is transmitted to the enforcement point rather than the policy template to substantially minimize use of data processing and communication resources (i.e., 411) [Fig. 5] [Figs. 1-4, 13-14 & 17] [col 1, L65 – col 2, L26];

determining if a policy template is present at an enforcement point (Policy Enforcers 142 / 126) [Fig. 1] [col 1, L65 – col 2, L26] in response to receiving an identification (ID) (i.e., Policy Identifier {ID}) [col 10, L53] assigned to the policy template at the enforcement point; (Menditto)

transmitting a query from the enforcement point to a repository, where policy templates are stored, in response to the policy template not being present at the enforcement point, wherein the query includes the ID assigned to the policy template; (Menditto)

receiving the policy template at the enforcement point, wherein the policy template is transmitted by the repository in response to the query; (Menditto) and

receiving a set of parameters (i.e., attributes) [col 19, L49-65] to be used in the policy template (e.g., selected policy enforcer 'settings') [Abstract] [Fig. 5] [col 8, L20-54] at the enforcement point (i.e., 411) [Fig. 5] [Figs. 1-4, 13-14 & 17] [col 1, L65 – col 2, L26].

While Shanumgam discloses substantial features of the invention, such as Policy Server Database 130, Policy Enforcement Points 124 / 126, Policy Settings for the Policy Enforcers, and Policy Identifier (ID) Attribute 724 for identifying a particular policy rule in the list of policies, and a method of distributing / replicating the 'policies' (including their Policy ID) from Policy Server to Policy Enforcers 124 / 126, the additionally recited features of the method comprising the steps of determining if a policy template is present at an enforcement point in response to receiving an identification (ID) assigned to the policy template at the enforcement point; transmitting a query from the enforcement point to a repository, where policy templates are stored, in response to the policy template not being present at the enforcement point, wherein the query includes the ID assigned to the policy template; and receiving the policy template at the enforcement point, wherein the policy template is transmitted by the repository in response to the query are disclosed by Menditto in a related endeavor.

Menditto discloses as his invention an information service provider network that includes a content gateway to process requests for information from a client terminal. The content gateway includes a router for receiving a request for information from the

client terminal. The router forwards the request according to the domain name to a selected one of a plurality of processors to further process the request. The selected one of the plurality of processors identifies an information source to satisfy the request in response to the additional content of the request [Abstract] [col 1, L45-53] [Figs. 1 & 3]. As part of his invention, Menditto discloses that "Content Gateways 18 distribute information from content providers 14 either directly or through content delivery nodes 22 to client terminals 16 according to Content Gateway Policy Manager 26 (CGPM). CGPM 26 is a management node in information service provider 12 that serves as a repository for content policies and communicates with content gateways 18 to distribute content policies within information service provider 12 and exchange policies with other CGPMs in other information service providers" [col 2, L43-53].

In particular, Menditto discloses the additionally recited features of the method comprising the steps of determining if a policy template is present at an enforcement point in response to receiving an identification (ID) assigned to the policy template at the enforcement point; transmitting a query from the enforcement point to a repository, where policy templates are stored, in response to the policy template not being present at the enforcement point, wherein the query includes the ID assigned to the policy template; and receiving the policy template at the enforcement point, wherein the policy template is transmitted by the repository in response to the query [col 3, L1-29][col 6, L16-53] (e.g., "...content policy may be *downloaded* to content gateway 18 *on-demand*....") [col 7, L1-53] [col 8, L27-30] (e.g., "...content policy associated with a

query...receiving policy updates from CGPM 26 and processing subsequent requests according to the newly installed policy.) [col 9, L37-62] [col 12, L20 –col 13, L6].

It would thus be obvious to one of ordinary skill in the art at the time of the invention to combine and/or modify Shanumgam's invention with the above said additionally recited features, as disclosed by Menditto for the motivation of providing systems and method for processing a request for information in a network that has considerable advantages over conventional routing techniques (e.g. determining a source of information based on the additional content of a request apart from the domain name associated therewith) [col 1, L54 – col 2, L2].

As per Claims 25, Shanumgam discloses the system of claim 23, wherein each enforcement point comprises:

a processor to receive the IDs assigned to each policy template (policy server 122 / policy enforcers 124 / 126) [Fig. 1] .

; and

a data source to store each policy template for enforcement and assigned ID, wherein the processor forms and transmits a query in response to each policy template corresponding to any transmitted IDs not present in the data source (e.g., repositories 130, 132, 134) [Fig. 1] [Figs. 3-4 & 12-19]

As per Claims 27, Shanumgam discloses the system of claim 26, further comprising a server to interface between each policy administrator, each enforcement point and the repository [Fig. 1].

3. Claims 6, 18, 32 and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shanumgam et al (hereinafter Shanumgam), U.S. Patent US 7,032,022 B1 in view of Menditto et al (hereinafter Menditto), U.S. Patent 6,981,029 and in further view of Widegren et al (hereinafter Widegren), U.S. Patent 6,621,793.

As per Claims 6, 18, 32 and 41, Shanumgam in view of Menditto and in further view of Widegren discloses the method of claim 1, further comprising applying asynchronous, out-of-band communication to transmit the query and any policy templates.

While the combination of Shanumgam and Menditto discloses substantial features of the invention such as the method of claim 5, and transmitting of policy templates in response to a query from the enforcement points, the added feature of the method further comprising applying asynchronous, out-of-band communication to transmit the query and any policy templates is disclosed by Widegren in a related endeavor.

Widegren discloses as his invention a method of filtering and gating data flow in a QoS connection between a remote host and user equipment in a packet data network using policy control mechanisms includes a remote host initiating an application in an application server and a corresponding session between the remote host and the user equipment ("UE") via the application server. The UE requests, to a gateway support node ("GGSN") of the network, establishment of a network bearer service between the UE and the remote host. A corresponding policy control function ("PCF") in a policy server receives, from the application server, filtering data derived from session data received by the application server during the session. The GGSN interrogates the corresponding PCF in the policy server to initialize a gate using policy control filtering data at the GGSN. The gate then filters the data flow in the QoS connection according to the policy control filtering data [Abstract]. In particular, Widegren discloses the added feature of the method further comprising applying asynchronous, out-of-band communication to transmit the query and any policy templates (e.g., asynchronous notification) [col 22, L41-53].

It would thus be obvious to one of ordinary skill in the art at the time of the invention to modify the combination of Shanumgam and Menditto's invention with the added feature of the method further comprising applying asynchronous, out-of-band communication to transmit the query and any policy templates, as disclosed by Widegren, for the motivation of providing a method of filtering and gating data in packet data networks using policy mechanisms [col 1, L15-17].

4. Claims 7, 19, 20, 33 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shanumgam et al (hereinafter Shanumgam), U.S. Patent US 7,032,022 B1 in view of Menditto et al (hereinafter Menditto), U.S. Patent 6,981,029 and in further view of and in further view of Danieli, U.S. Patent 6,510,513.

As per Claims 7, 19, 20, 33 and 42, Shanumgam view of Menditto and in further view of Danieli discloses the method of claim 1, further comprising compressing each policy template before transmitting to the enforcement point or any of the selected enforcement points.

While the combination of Shanumgam and Menditto discloses substantial features of the invention such as the method of claim 5, and transmitting of policy templates in response to a query from the enforcement points, the added feature of the method further comprising compressing each policy template before transmitting to the enforcement point or any of the selected enforcement points is disclosed by Danieli in a related endeavor.

Danieli discloses as his invention a Security services and policy enforcement for electronic data. A first client generates a digest from the electronic data, and submits a security certificate request containing the digest to a trusted arbitrator server, where the request is time stamped and logged. The trusted arbitrator authenticates the first client's credentials and returns the security certificate to the first client. The data and

security certificate are combined to create a distribution unit. A second client acquires the distribution unit, extracts the security certificate, and generates a digest from the data. If the digest from the second client matches the logged digest from the first client, the data is valid. Depending on the certificate type and policy level, the trusted arbitrator server provides other services to the clients, such as notification of improper user of the data [Abstract]. In particular, Danieli discloses the added feature of the method further comprising compressing each policy template before transmitting to the enforcement point or any of the selected enforcement points [col 16, L21-36].

It would thus be obvious to one of ordinary skill in the art at the time of the invention to modify the combination of Shanumgam and Menditto's invention with the added feature of the method further comprising compressing each policy template before transmitting to the enforcement point or any of the selected enforcement points, as disclosed by Danieli, for the motivation of providing a system and method for authenticating and validating electronic data and enforcing restrictions (e.g. policies) on the use of electronic data [col 1, L5-10].

5. Claims 8, 9, 21, 22, 34, 43 and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shanumgam et al (hereinafter Shanumgam), U.S. Patent US 7,032,022 B1 in view of Menditto et al (hereinafter Menditto), U.S. Patent 6,981,029 and in further view of Valente et al (hereinafter Valente), U.S. Patent Publication US 2003/0110192 A1.

As per Claims 8, 21, 34 and 43, Shanumgam in view of Menditto and in further view of Valente discloses the method of claim 1, further comprising forming the policy template in a structured document.

While the combination of Shanumgam and Menditto discloses substantial features of the invention such as the method of claim 5, and transmitting of policy templates in response to a query from the enforcement points, the added feature of the method further comprising forming each policy template in a structured document (e.g., XML document) is disclosed by Valente in a related endeavor.

Valente discloses as his invention a Security services and policy enforcement for electronic data. A first client generates a digest from the electronic data, and submits a security certificate request containing the digest to a trusted arbitrator server, where the request is time stamped and logged. The trusted arbitrator authenticates the first client's credentials and returns the security certificate to the first client. The data and security certificate are combined to create a distribution unit. A second client acquires the distribution unit, extracts the security certificate, and generates a digest from the data. If the digest from the second client matches the logged digest from the first client, the data is valid. Depending on the certificate type and policy level, the trusted arbitrator server provides other services to the clients, such as notification of improper user of the data [Abstract]. In particular, Valente discloses the added feature of the

method further comprising forming each policy template in a structured document [Abstract] (e.g., XML file 602a) [Fig. 6].

It would thus be obvious to one of ordinary skill in the art at the time of the invention to modify the combination of Shanumgam and Menditto's invention with the added feature of the method further comprising forming each policy template in a structured document (e.g., XML document), as disclosed by Valente, for the motivation of providing a system and method for authenticating and validating electronic data and enforcing restrictions (e.g. policies) on the use of electronic data [col 1, L5-10].

As per Claims 9, 22 and 44, Shanumgam in view of Menditto and in further view of Valente discloses the method of claim 1, further comprising forming the policy template in a mark-up language.

While the combination of Shanumgam and Menditto discloses substantial features of the invention such as the method of claim 5, and transmitting of policy templates in response to a query from the enforcement points, the added feature of the method further comprising forming each policy template in a mark-up language is disclosed by Valente in a related endeavor.

Valente discloses as his invention a Security services and policy enforcement for electronic data. A first client generates a digest from the electronic data, and submits a security certificate request containing the digest to a trusted arbitrator server, where the request is time stamped and logged. The trusted arbitrator authenticates the first

client's credentials and returns the security certificate to the first client. The data and security certificate are combined to create a distribution unit. A second client acquires the distribution unit, extracts the security certificate, and generates a digest from the data. If the digest from the second client matches the logged digest from the first client, the data is valid. Depending on the certificate type and policy level, the trusted arbitrator server provides other services to the clients, such as notification of improper user of the data [Abstract]. In particular, Valente discloses the added feature of the method further comprising forming each policy template in a mark-up language [Abstract] (e.g., XML file 602a) [Fig. 6].

It would thus be obvious to one of ordinary skill in the art at the time of the invention to modify the combination of Shanumgam and Menditto's invention with the added feature of the method further comprising forming each policy template in a structured document (e.g., XML document), as disclosed by Valente, for the motivation of providing a system and method for authenticating and validating electronic data and enforcing restrictions (e.g. policies) on the use of electronic data [col 1, L5-10].

Conclusion


1. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office Action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP 706.06(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

1. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Glenford Madamba whose telephone number is 571-272-7989. The examiner can normally be reached on M-F 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Valencia Wallace Martin can be reached on 571-272-3440. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

 JOHN FOLLANSBEE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Glenford Madamba
Examiner
Art Unit 2151